APPENDIX A

```
IF (it is time to perform housekeeping activities) THEN
    FOR (each TCP connection that has started to close, i.e. observed the TCP FIN flag set) DO
        IF (the time allowed for closure has passed) THEN
            Close this connection

            IF (this is the last connection with this user) THEN
                Reinitialize the user's profile and set the profile state to Incomplete
            ENDIF
        ENDIF
    NEXT

    FOR (each connection that has been idle for the maximum allowed time) DO
        Close this connection

        IF (this is the last connection with this user) THEN
            Reinitialize the user's profile and set the profile state to Incomplete
        ENDIF
    NEXT
ENDIF

IF (it is an IP packet) THEN
    IF (it is an IP/UDP packet) THEN
        Check the source and destination ports against a list of allowed well-known UDP ports

        IF (either port is on the allowed port list) THEN
            IF (the server port is for the XDMCP protocol) THEN
                Check the XDMCP Opcode against a list of allowed opcodes

                IF (the XDMCP Opcode is on the allowed opcode list) THEN
```

```
Check if the XDMCP packet is being sent in an allowed direction

IF (an allowed Opcode is being sent to the server or an allowed Opcode is being sent to the user) THEN
    IF (there is an established X-Windows connection with this user) THEN
        IF (the Opcode is other than KeepAlive or Alive) THEN
            Discard the packet
        ENDIF
    ELSE
        IF (the Opcode is KeepAlive or Alive) THEN
            Discard the packet
        ENDIF
    ENDIF

    Create and initialize a profile for this user

    Set the profile state to Incomplete

    IF (the Opcode is Query) THEN
        Reinitialize the user's profile and set the profile state to Incomplete

        FOR (each Authentication Name in the packet) DO
            IF (the Authentication Name is not recognized) THEN
                Discard the packet
            ENDIF
        NEXT

        Remember the Authentication Names in the user's profile

    ELSE IF (the Opcode is Willing) THEN
        IF (the Authentication Name in the packet is not recognized) THEN
            Discard the packet
        ENDIF
```

```
        IF (the Authentication Name is not one of the authentication names recorded in the user's
        profile from the Query packet) THEN
            Discard the packet
        ENDIF

        Remember this Authentication Name in the user's profile

        IF (the Hostname supplied by the server is NOT syntactically valid) THEN
            Discard the packet
        ENDIF

        IF (the Status string is NOT composed of printable characters) THEN
            Discard the packet
        ENDIF

    ELSE IF (the Opcode is Unwilling) THEN
        IF (the Hostname supplied by the server is NOT syntactically valid) THEN
            Discard the packet
        ENDIF

        IF (the Status string is NOT composed of printable characters) THEN
            Discard the packet
        ENDIF

        Reinitialize the user's profile and set the profile state to Incomplete

    ELSE IF (the Opcode is Request) THEN
        IF (the X Display Number is invalid) THEN
            Discard the packet
        ENDIF
```

```
Remember this Display Number in the user's profile

FOR (each Connection Type in the packet) DO
        IF (the Connection Type is not IP) THEN
                Discard the packet
        ENDIF
NEXT

FOR (each Connection Address in the packet) DO
        IF (the Connection Address is not an IP address) THEN
                Discard the packet
        ENDIF

        IF (the Connection Address does not match the user's IP address) THEN
                Replace the Connection Address with the user's IP address
        ENDIF
NEXT

IF (none of the Connection Addresses matched the user's IP address) THEN
        Discard the packet
ENDIF

IF (the Authentication Name in the packet is not recognized) THEN
        Discard the packet
ENDIF

IF (the Authentication Name does not match the Authentication Name recorded in the user's
profile from the Willing packet) THEN
        Discard the packet
ENDIF
```

```
IF (the lengths of the Authentication Name and Authentication Data are not both zero or
non-zero) THEN
        Discard the packet
ENDIF

FOR (each Authorization Name in the packet) DO
        IF (the Authorization Name is not recognized) THEN
                Discard the packet
        ENDIF
NEXT

Remember the Authorization Names in the user's profile

IF (if the Manufacturer Display ID contains invalid characters) THEN
        Discard the packet
ENDIF

IF (if the Manufacturer Display ID does not match any previous recorded Display ID for this
user) THEN
        Discard the packet
ENDIF

ELSE IF (the opcode is Accept) THEN
        Remember the Session ID in the user's profile

        IF (the Authentication Name in the packet is not recognized) THEN
                Discard the packet
        ENDIF

        IF (the Authentication Name does not match the Authentication Name recorded in the user's
        profile from the Request packet) THEN
                Discard the packet
```

```
        ENDIF

        IF (the lengths of the Authentication Name and Authentication Data are not both zero or
        non-zero) THEN
            Discard the packet
        ENDIF

        IF (the Authorization Name in the packet is not recognized) THEN
            Discard the packet
        ENDIF

        IF (the Authorization Name does not match any of the Authorization Names recorded in the
        user's profile from the Request packet) THEN
            Discard the packet
        ENDIF

        Remember the Authorization Name in the user's profile

        IF (the lengths of the Authorization Name and Authorization Data are not both zero or non-
        zero) THEN
            Discard the packet
        ENDIF

    ELSE IF (the opcode is Decline) THEN
        IF (the Status string is NOT composed of printable characters) THEN
            Discard the packet
        ENDIF

        IF (the Authentication Name in the packet is not recognized) THEN
            Discard the packet
        ENDIF
```

```
        IF (the Authentication Name does not match the Authentication Name recorded in the user's
        profile from the Request packet) THEN
            Discard the packet
195     ENDIF

        IF (the lengths of the Authentication Name and Authentication Data are not both zero or
        non-zero) THEN
            Discard the packet
200     ENDIF

        Reinitialize the user's profile and set the profile state to Incomplete

    ELSE IF (the opcode is Manage) THEN
205     IF (the Session ID does not match the Session ID recorded in the user's profile from the
        Accept packet) THEN
            Discard the packet
        ENDIF

210     IF (the X Display Number is invalid) THEN
            Discard the packet
        ENDIF

        IF (the Display Number does not match the Display Number recorded in the user's profile
215     from the Request packet) THEN
            Discard the packet
        ENDIF

        IF (if the Display Class contains invalid characters) THEN
220         Discard the packet
        ENDIF
```

```
        IF (if the Display Class does not match any previous recorded Display Class for this user)
        THEN
225         Discard the packet
        ENDIF

        Set the user's profile state to Complete

230 ELSE IF (the opcode is Refuse) THEN
        IF (the Session ID does not match the Session ID recorded in the user's profile from the
        Accept packet) THEN
            Discard the packet
        ENDIF
235
    ELSE IF (the opcode is Failed) THEN
        IF (the Session ID does not match the Session ID recorded in the user's profile from the
        Accept packet) THEN
            Discard the packet
240     ENDIF

        IF (the Status string is NOT composed of printable characters) THEN
            Discard the packet
        ENDIF
245
        Reinitialize the user's profile and set the profile state to Incomplete

    ELSE IF (the opcode is KeepAlive) THEN
        IF (the X Display Number is invalid) THEN
250         Discard the packet
        ENDIF

        IF (the Display Number does not match the Display Number recorded in the user's profile
        from the Manage packet) THEN
```

```
                    Discard the packet
                ENDIF

                IF (the Session ID does not match the Session ID recorded in the user's profile from the
                Manage packet) THEN
                    Discard the packet
                ENDIF

            ELSE IF (the opcode is Alive) THEN
                IF (the Session Running flag is not 0 or 1) THEN
                    Discard the packet
                ENDIF

                IF (the Session Running flag is True) THEN
                    IF (the Session ID does not match the Session ID recorded in the user's profile from
                    the Manage packet) THEN
                        Discard the packet
                    ENDIF
                ELSE – the Session Running flag is False
                    IF (the Session ID is not zero) THEN
                        Discard the packet
                    ENDIF

                    Reinitialize the user's profile and set the profile state to Incomplete
                ENDIF

            ELSE – the XDMCP Opcode is not allowed
                Discard the packet
            ENDIF
        ELSE – the XDMCP Opcode is being sent in the wrong direction
            Discard the packet
        ENDIF
```

```
                        ELSE – the XDMCP Opcode is not on the allowed-opcodes list
                            Discard the packet
                        ENDIF
290                 ELSE – the server port is not for the XDMCP protocol
                        Discard the packet
                    ENDIF
                ELSE – neither of the IP ports are on the allowed-ports list
                    Discard the packet
295             ENDIF

        ELSE IF (it is an IP/TCP packet) THEN
            IF (this packet is for an established TCP connection) THEN
                IF (the TCP RST flag is set) THEN
300                 Close this connection immediately

                    IF (this is the last connection with this user) THEN
                        Reinitialize the user's profile and set the profile state to Incomplete
                    ENDIF
305
                ELSE IF (the TCP FIN flag is set for the first time for this connection) THEN
                    Remember that the FIN flag was set in the user's profile

                    Record that the FIN flag was observed at the current date/time
310             ENDIF
            ELSE – the packet is not for an established TCP connection
                IF (the packet TCP SYN flag is set and the TCP ACK flag is not set) THEN
                    Check the source and destination ports against a list of allowed well-known TCP ports

315                 IF (either port is on the allowed port list) THEN
                        Check if the TCP connection is being opened in an allowed direction, i.e. the SYN packet is from the
                        server to an allowed user port or from the user to an allowed server port
```

```
                    IF (the TCP connection is being opened in an allowed direction) THEN
                        Check if the user port is for the X-Windows protocol

                        IF (this is an X-Windows connection) THEN
                            IF (there is not an existing profile for this user) THEN
                                Discard the packet
                            ELSE – there is an existing profile for this user
                                IF (the state of the user's profile is not Complete) THEN
                                    Discard the packet
                                ENDIF

                                IF (the user port does not correspond to the X Display Number in the user's profile)
                                THEN
                                    Discard the packet
                                ENDIF
                            ENDIF
                        ENDIF

                        Remember this connection in the user's profile
                    ELSE – the TCP connection is being opened in a disallowed direction
                        Discard the packet
                    ENDIF
                ELSE – neither of the IP ports are on the allowed-ports list
                    Discard the packet
                ENDIF
            ELSE – this is not a TCP SYN packet
                Discard the packet
            ENDIF
        ENDIF

        Remember the current date/time as that of the last packet on this connection
    ELSE – it is neither and IP/UDP or IP/TCP packet
```

```
            Discard the packet
        ENDIF
    ELSE – it is a non-IP packet
        Discard the packet
355 ENDIF
```